Security Operations FortiManager Integration App - User Guide

Version 1.1 for FortiManager 6.0.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

July 6, 2018
Security Operations FortiManager Integration App 1.1 for FortiManager 6.0.1 User Guide
02-601-496728-20180706

TABLE OF CONTENTS

Overview

You can use the Security Operations FortiManager Integration App on ServiceNow to push configuration changes to FortiManager either automatically or manually. You can also use the Security Operations FortiManager Integration App on ServiceNow with other ServiceNow apps and services.

Users can use the Security Operations FortiManager Integration App on ServiceNow to:

- Respond to security incidents.
- Contain security threats by quarantining endpoints or blocking certain network traffic.

Administrators can use the Security Operations FortiManager Integration App on ServiceNow to:

- Deploy configuration changes to different FortiGate firewalls through FortiManager.
- Create configuration templates to use for change requests.
- Approve configuration change requests and push the changes to FortiManager.
- Track configuration change deployment to FortiManager.

The Security Operations FortiManager Integration App on ServiceNow is available in the ServiceNow Store. See Download the app on page 6.

Additional information

For more information, see the FortiManager release notes in the Fortinet Document Library.

For information on using FortiManager, see the FortiManager *Administration Guide* in the Fortinet Document Library.

For general best practices on using FortiManager, see the FortiManager *Best Practices* in the Fortinet Document Library.

Requirements

ServiceNow requirements

Your organization must have a ServiceNow subscription that includes credentials to log in to ServiceNow to download and use ServiceNow apps, including the Security Operations FortiManager Integration App.

Security Operations FortiManager Integration App parameters

The Security Operations FortiManager Integration App is supported for desktop use in English and is recommended for use within the following parameters:

Maximum ADOMs	5
Maximum FortiGates per ADOM	100
Maximum policy packages per ADOM	20
Maximum installation targets per policy package	100
Maximum objects per ADOM	20 schedules, 100 services, 800 addresses, 80 interfaces

Set Up and Configuration

To use the Security Operations FortiManager Integration App:

1. In FortiManager, set up an administrator account for the Security Operations FortiManager Integration App. See Set up FortiManager for the app on page 6.
2. In FortiManager, set up a certificate for the Security Operations FortiManager Integration App. See Set up FortiManager for the app on page 6.
3. In FortiManager, set up JSON-RPC permissions for the Security Operations FortiManager Integration App. See Set up JSON-RPC permission in FortiManager on page 6.
4. In ServiceNow, download the Security Operations FortiManager Integration App. See Download the app on page 6.
5. Configure the Security Operations FortiManager Integration App. See Configure the app on page 7.

Set up FortiManager for the app

- Create or select a FortiManager administrator account that you want to use for integration with the app. This account does not require a Super_User administrator profile and the *Trusted Hosts* field does not need to be turned on.

  For more information, see the FortiManager *Administration Guide* in the Fortinet Document Library.
- The Security Operations FortiManager Integration App requires trusted SSL certificates to be installed in FortiManager for secure API communication. See the *Certificates* section in the *FortiManager Administration Guide*.

Set up JSON-RPC permission in FortiManager

To set up JSON-RPC permission in FortiManager using CLI commands:

1. Using CLI or in the *Dashboard* > *CLI Console* widget, set the JSON-RPC permission:

```
config system admin user
edit servicenow_account
   set rpc-permit read-write
end
```

Download the app

Your organization must have a ServiceNow subscription that includes credentials to log in to ServiceNow to download and use ServiceNow apps, including the Security Operations FortiManager Integration App. For more information, see the online help in https://store.servicenow.com.

To download the Security Operations FortiManager Integration App:

1. Go to the ServiceNow store at https://store.servicenow.com.
2. Search for Security Operations FortiManager Integration and click *Get*.
3. Follow the onscreen instructions to download the Security Operations FortiManager Integration App.

After downloading the Security Operations FortiManager Integration App, add it to the *Favorites* menu for easy access.

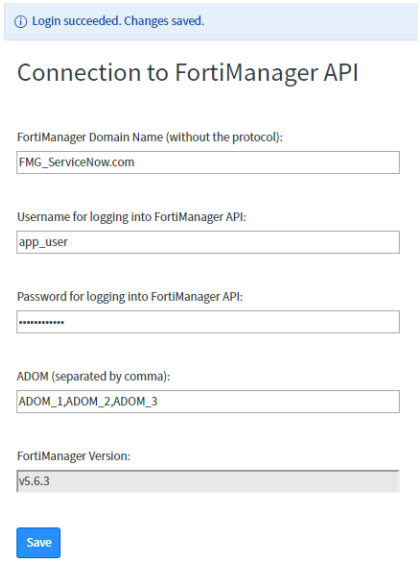
Configure the app

To configure the Security Operations FortiManager Integration App:

1. Open the *Security Operations FortiManager Integration App* in a web browser and go to *FortiManager App* > *FMG System Properties*.
2. Enter the information for connecting to the FortiManager API:
   - The FortiManager domain name without the protocol, for example, `FMG_ServiceNow.com`.
   - The username of the FortiManager account to use with ServiceNow.
   - The password of the FortiManager account to use with ServiceNow.
   - The FortiManager ADOMs you want to access, each separated by a comma.

   Ensure the FortiManager ADOM names are spelled correctly.
3. Click *Save*.

A login success message displays at the top and the *FortiManager Version* displays at the bottom. This indicates that the app is communicating with FortiManager and shows the FortiManager version at the bottom.



Using the Security Operations FortiManager Integration App

Use the Security Operations FortiManager Integration App to do the following:

- Create change requests.
- Track change requests.
- Create configuration templates.
- Modify configuration templates.
- Configure the connection to FortiManager. See Configure the app on page 7.

FortiManager Configuration Templates

You can create change requests without using a template.

Using a template helps you to create change requests more easily by filling in relevant information for that template type. You can create custom templates or use a predefined template type.

The FortiManager Security Operations FortiManager Integration App includes the following predefined template types:

Template Type	Description
IPv4 Deny Policy	Template to create an IPv4 Deny Policy on FortiGates.
Quarantine MAC Address	Template to command FortiGate to quarantine a MAC address.

To create or modify a FortiManager config template:

1. Go to *FortiManager app* > *FMG Config Templates*.
   - To create a template, click *New* in the toolbar.
   - To modify a template, click the template name.
2. Enter or modify the template information and click *Submit* or *Update*.

FortiManager Change Requests

You can create a change request manually or from an incident.

When creating a change request from an incident, the incident details are already entered. You just have to enter the other required fields such as the template name and MAC address.

To manually create a FortiManager change request:

1. Go to *FortiManager app* > *FMG Change Requests*.
2. Click New and enter the change request information.
3. Scroll down and click the *FortiManager* tab, select the *Template Name* and fill in the required fields.
4. Click *Submit*.

The change request is created but not yet approved.

To approve a change request:

1. Go to *FortiManager app* > *FMG Change Requests*.
2. Click the request number you want to approve.
3. Change the *Approval* field to *Approved*.
4. Click *Update*.

FortiManager Configuration Change Trackers

The *FortiManager app* > *FMG Config Change Trackers* shows the status of approved change requests.

To see details of the change, click the *Number*.

Change requests that have been delivered to FortiManager show *Completed* in the *Implementation Status* column.

The *FMG Task ID* matches the FortiManager *System Settings* > *Task Monitor ID* field. You can task status in both *FortiManager app* > *FMG Config Change Trackers* and *FortiManager* > *System Settings* > *Task Monitor*.

Troubleshooting

Connection issues between FortiManager and the app

To troubleshoot connection issues between FortiManager and the Security Operations FortiManager Integration App:

1. In FortiManager, go to *System Settings* > *Admin* > *Administrators*.
   a. Click the ServiceNow account and check that settings are correct.
      See Set up FortiManager for the app on page 6.
2. Check that you have set up JSON-RPC permission correctly.
   See Set up JSON-RPC permission in FortiManager on page 6.
3. In the *Security Operations FortiManager Integration App*, go to *FortiManager app* > *FMG System Properties*.
   a. Check that the connection settings are correct, especially the *FortiManager Domain Name* and ADOM names.
      See Configure the app on page 7.
      If connection settings are incorrect, the app displays an error message when you click *Save*.

Troubleshooting log message errors

In ServiceNow, click *All applications* and search for *system logs*. Then select *Application Logs*.

In the *App Log* pane, check for errors. You can filter by keywords to search for messages.

Log message type	Possible solutions
Login failed messages such as ***Login status: Failed - No permission for the resource***	Check that the domain name, username, and password are correct in both the app and FortiManager. See Set up FortiManager for the app on page 6.
HTTP error message: ***Unknown host***	Check that the domain name is correct and FortiManager is running.
SocketTimeoutException: connect timed out when posting to... and ***Login status: Failed - unknown***	Check that certificates are installed correctly on FortiManager. See Set up FortiManager for the app on page 6.
Login status: OK but Response body shows ***No permission for the resource***	Check that JSON-RPC permission is set to read-write. See Set up FortiManager for the app on page 6.

Configuration changes are not pushed to FortiManager

When a change request is approved, the configuration is pushed to FortiManager and you can see the status in *FMG Config Change Tracker*. In addition to being approved, a change request must use a valid configuration template before it can be pushed to FortiManager.

If a configuration change fails to be pushed to FortiManager, check the following:

- Check the connection between ServiceNow and FortiManager. See Connection issues between FortiManager and the app on page 10.
- Check that the change request is approved.
- Check that a valid configuration template is used; and the template type, installation target, and template fields are correct.
- For the *IPv4 Deny Policy* template type, if there are custom address objects, check that they follow the correct IP/subnet format.
- Check that the implementation status is *Completed* in *FMG Config Change Tracker*.
- Check the configuration installation status on FortiManager:
  a. In *FMG Config Change Trackers*, find the *FMG Task ID*.
  b. *In FortiManager* > *System Settings* > *Task Monitor*, find the task.
  c. Check the task *Status* to see if the configuration change is successfully installed in installation targets.

Troubleshooting other issues

Issue	Possible solutions
Cannot create or update *FMG Config Templates*	If *FMG Config Templates* has no **New** button, check that your account has `x_forti_fmgintg.fmg_templates_write` permission.
ADOMs do not appear in the dropdown list in the *FMG Config Templates* > *Installation Target* tab.	This applies to the *IPv4 Deny Policy* template type. If FortiManager has a large data set, ServiceNow takes longer to process the data. Wait and try again.
You get an error message after choosing an ADOM in the *FMG Config Templates* > *Installation Target* tab.	Check that all ADOMs in *FMG System Properties* are valid and spelled correctly.
Policy packages do not appear in the dropdown list in the *FMG Config Templates* > *Installation Target* tab.	This applies to the *IPv4 Deny Policy* template type. Check that the target policy package has *Installation Targets* set up in FortiManager.
Cannot access *FMG Change Requests* page or get errors using this page	Check that your account has `x_forti_fmgintg.fmg_change_request_requester` permission.
Cannot update *FMG System Properties*	Check that your account has `x_forti_fmgintg.fmg_system_property_write` permission.

Issue	Possible solutions
Cannot see records in *FMG Config Change Tracker*	Check that your account has `x_forti_fmgintg.fmg_config_change_tracker_read` permission.

Change Log

Date	Change Description
2018-07-06	Initial release.

Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.